

CLAIM

Pub 1. An offline-online points system, comprising:
2 a main server for providing a user with an interface to submit a code, wherein the user
3 obtained the code offline and the code is associated with N points; and
4 a code server for maintaining valid codes and verifying that the code that the user
5 submitted is a valid code.

1 2. The system of claim 1, further comprising:
2 a user database that maintains an account of the user, wherein the account balance is M
3 points prior to the user's submission of the code.

1 3. The system of claim 2, wherein the code server updates the account balance to M+N
2 points after the user submits the code and if the code server verifies that the code is valid.

1 4. The system of claim 2, wherein the main server updates the account balance to M+N
2 points after the user submits the code if the code server verifies that the code is valid.

1 5. The system of claim 2 wherein the code is C letters in length from an alphabet of L
2 letters.

1 6. The system of claim 5 wherein C is 10.

1 7. The system of claim 6 wherein L is 29.

1 8. The system of claim 6 wherein L is 36.

1 9. A method of generating an encrypted code in base L, comprising steps:
2 providing an n-bit raw number;
3 applying a one-way hash function on the n-bit raw number with a first secret key to
4 generate a first string;

5 designating an m-bit portion of the first string as an m-bit validation number; and
 6 combining the m-bit validation number and the n-bit raw number to generate a second
 7 string.

1 10. The method of claim 9, further comprising steps:
 2 applying a DES3 encryption algorithm to the second string with a second secret key to
 3 generate a third string; and
 4 converting the third string to base L to generate the encrypted code.

1 11. The method of claim 9, wherein $n=32$, $m=16$, and $L=29$.

1 12. The method of claim 9, wherein the one-way hash function is MD5.

1 13. The method of claim 9, wherein the step of combining includes:
 2 concatenating the m-bit validation number and the n-bit raw number.

1 14. The method of claim 13, wherein the m-bit validation number is the most significant bit
 2 (MSB) portion of the second string.

1 15. The method of claim 9, wherein the m-bit validation number is the m most significant
 2 bit (MSB) of the first string.

1 16. A method of verifying the validity of a code, comprising steps:
 2 generating a code with encrypted information;
 3 providing the code on a hard good to be distributed to users;
 4 receiving the code online; and
 5 verifying the validity of the code by processing the encrypted information.

1 17. The method of claim 16, wherein the step of generating includes steps:
 2 providing an n-bit raw number;
 3 applying a one-way hash function on the n-bit raw number with a first secret key to
 4 generate a first string;
 5 designating an m-bit portion of the first string as an m-bit validation number;

6 combining the m-bit validation number and the n-bit raw number to generate a second
 7 string;
 8 applying a DES3 encryption algorithm to the second string with a second secret key to
 9 generate a third string; and
 10 converting the third string to base L to generate the code with the encrypted
 11 information.

1 18. The method of claim 17, wherein the step of verifying includes:
 2 converting the code in base L to generate a first test code in base 2;
 3 decrypting the first test code with the second secret key using a reverse DES3
 4 encryption algorithm to generate a second test code;
 5 applying the one-way hash algorithm to the second test code to generate a third test
 6 code; and
 7 comparing a designated m-bit portion of the second test code to a designated m-bit
 8 portion of the third test code, and if the comparison is positive, declaring the code to be valid.

1 19. The method of claim 18, wherein the m-bit validation number is the m most significant
 2 bit (MSB) of the first string in the generating step and the designated m-bit portion is the most
 3 significant bit portion of the second test code and third test code in the comparing step.

1 20. A method for awarding incentive points to a user, comprising steps:
 2 generating a code with encrypted information;
 3 providing the code to an entity for printing on a hard good;
 4 receiving the code submitted by the user; and
 5 verifying the validity of the code by processing the encrypted information.

1 21. The method of claim 20, wherein the step of generating includes steps:
 2 providing an n-bit raw number;
 3 applying a one-way hash function on the n-bit raw number with a first secret key to
 4 generate a first string;
 5 designating an m-bit portion of the first string as an m-bit validation number;

